

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

FILED

AUG 14 2019

Clerk, U.S. District Court
Texas Eastern

UNITED STATES OF AMERICA

§
§
§
§
§

SEALED

v.

Case No. 4:19CR 181

Judge *Mazzant*

CONRAD ROCKENHAUS

INDICTMENT

THE UNITED STATES GRAND JURY CHARGES:

Count One

Violation: 18 U.S.C. §
1030(a)(5)(A) (Intentional
Damage to a Protected Computer)

Introduction

At all times material to this Indictment:

1. The victim in this case (hereinafter, "Victim Company") was an online company providing travel booking and vacation services to customers. Victim Company maintained a regional office and operated a computer network with servers located in Collin County, Texas, in the Eastern District of Texas.

2. Defendant CONRAD ROCKENHAUS was employed as a developer services manager, and later an infrastructure architect, for Victim Company beginning on or around February 28, 2014. In these roles, ROCKENHAUS managed both development and production servers running the Victim Company's website and was responsible for the network infrastructure and associated security. During his employment with Victim

Company, ROCKENHAUS resided in Denton County, Texas, in the Eastern District of Texas.

3. Victim Company's online production and development environments were located on multiple computer servers residing in data centers in different parts of the United States. These servers contained computer code that controlled several business functions for the Victim Company, including marketing, scheduling, and payment processing. Users, including ROCKENHAUS, could connect to Victim Company's servers remotely using a Virtual Private Network ("VPN") employing multi-factor authentication.

4. ROCKENHAUS was terminated from Victim Company on or about November 10, 2014.

The Offense

A. Conrad Rockenhaus' Unauthorized Access to Victim Company's Computers

5. On or about November 11, 2014, shortly after ROCKENHAUS was terminated by Victim Company, ROCKENHAUS remotely accessed the servers via VPN from his residence located in Denton County, Texas, in the Eastern District of Texas. Because ROCKENHAUS could not gain privileged access to the system utilizing a traditional administrative account, he used an account he created prior to his termination in order to gain "superuser access" to Victim Company's servers (also known in the industry as a "back door").

6. After gaining administrative access to the Victim Company's servers, ROCKENHAUS executed a command to shut down a Logical Unit Number ("LUN") on

one of the Victim Company's servers, which in turn caused several other Victim Company's servers to crash.

7. Not knowing ROCKENHAUS's involvement in the server crash, Victim Company contacted ROCKENHAUS to help restore its servers shortly after the crash. Victim Company's management viewed ROCKENHAUS as someone who understood the network infrastructure and could facilitate the quickest recovery. In the days following Victim Company's server crash, ROCKENHAUS was granted access to the Victim Company's network to assist with recovery. Victim Company agreed to pay ROCKENHAUS as a contractor for these services.

8. During its remediation efforts, Victim Company continued its investigation of the crash and began to suspect ROCKENHAUS's involvement with the server crash. On or about November 16, 2014, Victim Company terminated its contractual agreement to have ROCKENHAUS assist with the server reconstitution, and notified ROCKENHAUS of that termination.

9. Over the course of the remediation efforts, ROCKENHAUS entered the disaster recovery facility, located in Plano, Texas, in the Eastern District of Texas, with other company personnel. However, on or around November 21, 2014, unbeknownst to and without authorization from anyone at Victim Company, ROCKENHAUS re-entered the Plano facility alone and disconnected several servers and removed them from the rack, replacing the rack's faceplate.

10. As a result of the multiple server shutdowns caused by ROCKENHAUS, Victim Company's business was not fully operational for approximately thirty cumulative hours between November 10, 2014 and November 24, 2014. During this time period, customers looking to book vacations or utilize Victim Company's travel services were unable to access Victim Company's website. In sum, the server shutdown caused by ROCKENHAUS cost Victim Company approximately \$242,775 in lost revenue and approximately \$321,858 in recovery and remediation costs.

B. Execution of the Offense

11. On or about November 11, 2014, within the Eastern District of Texas and elsewhere, the defendant, CONRAD ROCKENHAUS, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused, and attempted to cause, damage, without authorization, to a protected computer, to wit, by logging into Victim Company's servers after his termination of employment, executing a command to shut down Victim Company's servers, and the offense caused loss during a 1-year period aggregating at least \$5,000 in value.

All in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i).

NOTICE OF INTENT TO SEEK CRIMINAL FORFEITURE

1. The allegations contained in Count One of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

2. Upon conviction of the computer fraud offense in violation of Title 18, United States Code, Section 1030, set forth in Count One of this Indictment, defendant CONRAD ROCKENHAUS shall forfeit to the United States of America:

- a. Pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of such offense;
and
- b. Pursuant to Title 18, United States Code, Section 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such offense. The property to be forfeited includes, but is not limited to:
 1. Phones, computers, or electronic devices used in the commission of the offense; and
 2. A sum of money equal to the proceeds derived from or obtained as a result of such offense.

3. If any of the property described above, as a result of any act or omission of the defendant:

- a. Cannot be located upon the exercise of due diligence;
- b. Has been transferred or sold to, or deposited with, a third party;
- c. Has been placed beyond the jurisdiction of the court;
- d. Has been substantially diminished in value; or
- e. Has been commingled with other property which cannot be divided without difficulty,


the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b) and 1030(i).

A TRUE BILL:

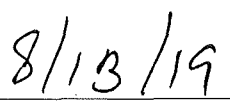


GRAND JURY FOREPERSON

JOSEPH D. BROWN
UNITED STATES ATTORNEY
EASTERN DISTRICT OF TEXAS



Anand Varadarajan
Assistant United States Attorney



Date

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

UNITED STATES OF AMERICA

§
§
§
§
§

SEALED

v.

Case No. 4:19CR 181

Judge Mazzant

CONRAD ROCKENHAUS

NOTICE OF PENALTY

Count One

Violation: 18 U.S.C. § 1030(a)(5)(A)

Penalty: Not more than ten years imprisonment, a fine not to exceed \$250,000, or not more than the greater of twice the gross gain to the defendant or twice the gross loss to one other than the defendant, or both; supervised release of not more than three years.

Special

Assessment: \$100.00